



RISK ASSESSMENT CHECKLIST

Provided
By
The Office of the Georgia State Inspector General

Produced In Cooperation With
The Governor's Office of Texas

Fraud Risk Assessment Checklist

Performing an agency fraud risk assessment is a critical component of an agency's antifraud program. When agency management adds fraud to the list of potential risks it faces and assesses that risk, it will be more likely to identify potential fraud schemes and scenarios and better able to design effective controls to prevent and detect them. The fraud risk assessment should be performed in two steps:

- 1) Perform an agency-wide environmental infrastructure assessment or check-up. This section covers the "Key Components of a Fraud Prevention and Detection Program" document and addresses the tone at the top and the ethical culture at an agency.
- 2) Perform a detailed assessment by division, process, or core function. This section should include, at minimum, the following administrative functions and services:
 - Finance and Accounting
 - Purchasing and Contracting
 - License and or Permit Issuing
 - Financial Grant Management
 - Information Technology
 - Human Resources Management
 - Any Cash/Revenue Producing Function

Management should ensure that specific risks for fraud are included in the risk assessment process. The risk assessment process will result in the identification of agency activities, the risks associated with each activity, and the controls that are in place or should be in place to mitigate the risks.

COMPONENT	Y/N	COMMENTS/COMPENSATING CONTROLS IF ANSWER IS "NO"
I. Culture of Honesty and Ethics <ul style="list-style-type: none">• Setting the Tone at the Top:<ol style="list-style-type: none">1. <i>Is there a written Code of Conduct?</i><ol style="list-style-type: none">a) Is the Code of Conduct disseminated to all employees at time of hire?b) Is there at least annual refresher training on the code of conduct for every employee?c) Is there a method of determining that employees understand the contents of		

COMPONENT	Y/N	COMMENTS/COMPENSATING CONTROLS IF ANSWER IS "NO"
<p>the code of conduct?</p> <p>d) Do employees have a communication avenue for asking questions when ethical situations arise?</p> <p>2. <i>Is there a Confidential Reporting Mechanism for employees to use to report suspected or possible fraud without fear of reprisal?</i></p> <p>a) Is the Confidential Reporting Mechanism contact widely advertised so that all employees are aware of it?</p> <p>b) Is there a protocol for handling all Confidential Reporting Mechanism activity?</p> <p>c) Is activity of the Confidential Reporting Mechanism reported to executive management and the board?</p> <p>• Creating a Positive Workplace Environment:</p> <p>1. <i>Is there an employee recognition and reward system or compensation program?</i></p> <p>2. <i>Is there a whistle blower policy, a system for employees to obtain advice internally before making decisions that have significant legal or ethical implications, and/or a process to encourage employees to communicate or report, on a confidential or anonymous basis, without fear of retribution, concerns related to wrongdoing or violations?</i></p> <p>• Hiring and Promoting Appropriate</p>		

COMPONENT	Y/N	COMMENTS/COMPENSATING CONTROLS IF ANSWER IS "NO"
<p>Employees:</p> <p><i>1. Are background checks, both criminal and work, performed on employees, especially those in positions of trust?</i></p> <ul style="list-style-type: none"> • Training: <p><i>1. Is there a mechanism for tracking employee training and understanding of the code of conduct?</i></p> • Notification and Confirmation: <p><i>1. Are employees held accountable for proactively addressing the potential of fraud in the discharge of their assigned duties?</i></p> <p>a) Are awareness of fraud and the management of fraud risks included in every managers (perhaps employees) personnel evaluation?</p> • Discipline: <p><i>1. Are there consequences for employees who commit fraud and are those consequences consistent and fair?</i></p> <p>a) Are consequences pre-determined, that is defined in a fraud policy?</p> <p>b) Is there a formal procedure for documenting the consequences of each proven fraud?</p> 		

<p>II. Antifraud Processes and Controls</p> <ul style="list-style-type: none"> • Identifying and Measuring Fraud Risks: 		
--	--	--

<ul style="list-style-type: none"> • Mitigating Fraud Risks: • Implementing and Monitoring Appropriate Internal Controls: <p>1. <i>Is risk assessment performed by each division, location, or segment separately?</i></p> <p>a) Are possible misconduct schemes, fraud scenarios, fraud categories, and applicable business activity or process identified? Examples:</p> <ul style="list-style-type: none"> • If you were the Controller for the agency, how could you embezzle funds, manipulate the financial records, and not get caught? • What various ways an insider or outsider can manipulate this process to commit fraud against the agency? <p>b) Were consequences posed by each scheme and were management's tolerance for risks considered?</p> <ul style="list-style-type: none"> • Reputation damage • Financial damage - Monetary loss • Legal damage – Criminal or civil sanctions <p>c) Were they documented?</p>		
<p>2. <i>Were red flags of fraud considered in the evaluation?</i></p> <ul style="list-style-type: none"> • Personal characteristics or situational pressures that can lead to fraud • Agency opportunities that can lead to fraud • Opportunities that allow or encourage management fraud 		

<p>3. Was the likelihood that each particular fraud will occur evaluated?</p> <ul style="list-style-type: none"> • Remote • Reasonably possible • Probable <p>4. Were direct or indirect controls applicable to above documented scenarios identified? Basic controls include:</p> <ul style="list-style-type: none"> • Segregation of duties relating to authorization, custody of assets, and recording and reporting of transactions • Supervisory reviews, verifications, reconciliation • Automated edit checks and system controls • Physical and logical security of assets • Embedded audit checks • Fraud detection software 		
--	--	--

<p>III. Appropriate Oversight Process</p> <ul style="list-style-type: none"> • Commission or Board of Directors: <p>1. Is there a communication mechanism by which executive management and the board is made aware of antifraud programs, controls, and results?</p> <p>a) Are they advised of the potential fraud risks in the agency?</p> <p>b) Are they made aware of the elements of the agency's antifraud programs and</p> 		
--	--	--

<p>controls?</p> <p>c) Are they advised of all actual frauds and the actions taken to mitigate future similar frauds?</p> <p>d) Are they advised of activity to the Confidential Reporting Mechanism?</p> <p>• Management:</p> <p><i>1. Is there a member of executive management designated as the responsible party or point of contact for the fraud prevention?</i></p> <p>a) Is this person the liaison with the Office of the Inspector General?</p> <p>b) Does this person provide continuous reinforcement of the antifraud programs to all employees?</p> <p>c) Is this person responsible directly to executive management and the board for the antifraud programs of the agency?</p>		
---	--	--

Sources

- Management Anti-fraud Programs and Controls commissioned by the Fraud Task Force of the American Institute of Certified Public Accountants, AICPA’ Auditing Standards Board.
- Key Elements of Anti-fraud Programs and Controls by Price Waterhouse Coopers
- Price Waterhouse Coopers article “The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risks”.
- Fraud Prevention Checkup by the Association of Certified Fraud Examiners
- SAO’s Internal Audit Best Practice List
- SAO Small State Agency Risk Assessment (HB 2485) Instructions
- SAO Fraud and Criminal Activity Questionnaire Overview
- Statement on Auditing Standards No. 99, Consideration of Fraud in a Financial Statement Audit